A

Synopsis

On

Study of Distance Properties of Certain Linear Codes

Submitted to

Swami Ramanand Teerth Marathwada University

Nanded-431606, Maharashtra State, India.

For Registration of (Ph.D) Doctor of Philosophy in Mathematics

Research Student

Mr. Sonkamble Rajesh Digambarrao

Under the Guidance of

Dr. Arun Baburao Jadhav

Associate Professor,

Head of Mathematics Department,

DSM College Parabhani.

Swami Ramanand Teerth Marathwada University,
Nanded-431606, Maharashtra, India.

1 Introduction

Digital communication across a noisy channel is proned to errors in communication. Error correcting codes overcome this difficulty and they not only detect the error but correct those errors upto certain extent. Therefore a good encoding scheme (construction of good codes) is the most vital part in the digital communication. One of the goal in coding theory is to develop systems and methods that allow to detect and correct errors caused when information is transmitted through noisy channels. Codes were initially developed to correct errors on noisy and inaccurate communication channels. This further motivates researchers to pay attention towards linear codes. Linear codes are simple to understand, yet are the most important and effective for practical applications, such as encoding and decoding messages sent over communication channels.
In my proposed work I would like to study distance properties of some of recently developed linear codes. A family of cyclic codes is one of my interests. This family of linear codes consists of Cyclic, Quasi-cyclic, Negacyclic and Constacyclic codes.

2 Review of literature and development in the subject

Claude Shannon is considered as the pioneer of the coding theory. In 1949 Shannon has published a paper *A Mathematical Theory of Communication*,[13] where Shannon has focused on encoding the information based on probabilitic approch. In 1949 Golay codes were developed which were able to correct 3 errors in 24 bit codeword. In 1950 Richard Hamming has developed automatic coding system to error detecting and error correcting codes[12]. Hamming has invented Hamming codes, Hamming distances, Hamming numbers.
In the transmisson of picture of the earth taken by satellite, for this purpose the picture is decompsed into pixels and each pixel has certain grey value. The grey value is then mapped to a number, which in turn is converted to a binary sequence by means of the binary representation of an integer. In the case of six values of grey, we have the messages 0, 1, 10, 11, 100, 101. By padding with zeros up-front, we can make the sequences all of have length 3. We can also add the remaining sequences of that length over the given alphabet, which in our case gives 000, 001, 010, 011, 100, 101, 110, 111. The two elements 0 and 1 are the elements of a field $\mathbb{F}_2$, the binary field. The above sequences can be considered as the vectors of $\mathbb{F}_2^3$, the three-dimensional vector space over $\mathbb{F}_2$. In more general situations it will be a $k-$dimensional vector space $\mathbb{F}^k$ over a finite field $\mathbb{F}$, which may be different from the field of two elements. Therefore, a field consisting of q elements is indicated by $\mathbb{F}_q$, where $q = p^m$ and p is a prime number. Let $\mathbb{F}_q$ be a finite field with

q elements where q is a power of prime p and $\mathbb{F}_q^n$ be the n dimensional vector space over $\mathbb{F}_q$. Then linear $[n,k]_q$ code of length n is a k dimensional subspace of $\mathbb{F}_q^n$. The vectors $(c_1, c_2, \cdots, c_n) \in C$ are called codewords. The number of non zero entries in a codeword $x = (c_1, c_2, \cdots, c_n)$ of C is called Hamming weight or Hamming norm and is denoted by $\|x\|$. The $\min\{\|x\| : x \in C\}$ is called Minimum Hamming weight or Minimum weight and is denoted by $d(C)$.

Cyclic codes are known to be a crucial subcategory of linear coding technique because these codes offers efficient encoding and decoding schemes. Various other important codes like, Reed-Solomon codes, Golay codes, Hamming codes, BCH codes belongs to family of cyclic codes. The proper context for studying cyclic codes of length n over the finite field $\mathbb{F}_q$ of order q, where $q = p^n$ and p a prime, is the residue class ring $R_n = \mathbb{F}_q[x]/(x^n - 1)$, where $(x^n - 1)$ denotes the ideal genrated by $x^n - 1 \in \mathbb{F}_q[x]$. A $[n,k]_q$ linear code C is said to be cyclic if it is linear and for every code word $(c_0, c_1, ..., c_{n-1}) \in C$, its right cyclic shift $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$. These cyclic codes possess the linearity and cyclic shift property. Each codeword $(c_0, c_1, ..., c_{n-1})$ is customarily identified with its polynomial representation $c_0 + c_1 x + ... + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Let $\sigma, \gamma, \& \tau$ be the maps from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ given by $\sigma(c_0, c_1, ...c_n) = (c_{n-1}, c_0, c_1, ...c_{n-2})$, $\gamma(c_0, c_1, ...c_n) = (-c_{n-1}, c_0, c_1, ...c_{n-2})$, $\tau(c_0, c_1, ...c_n) = (\lambda c_{n-1}, c_0, c_1, ...c_{n-2})$. Then C is said to be Cyclic, if $\sigma(C) = C$ and polynomial representation of C is ideal in $\mathbb{F}_q[x]/(x^n - 1)$. As defined above C is said to be negacyclic, if $\gamma(C) = C$ and polynomial representation of C is ideal in $\mathbb{F}_q[x]/(x^n + 1)$. C is said to be Constacyclic, if $\tau(C) = C$ and polynomial representation of C is ideal in $\mathbb{F}_q[x]/(x^n - \lambda)$ [16]. A code C is said to be quasi-cyclic if a cyclic shift of any codeword by p positions is still a codeword. Thus a cyclic code is a quasi-cyclic code with $p = 1$. The block length n of a quasi-cyclic code is a multiple of p, or $n = m \times p$.

Let A_i be the number of codewords with weight i in C of length n. The sequence $(1, A_1, ..., A_n)$ is referred as the weight distribution of C. If the number of nonzero A_i in the sequence $(A_1, ..., A_n)$ is equal to t, we call C a t-weight code. The weight distribution contains important information of a code. In classic coding theory, it gives the minimum distance of the code which determines the error correction capability of the code. Different kinds of linear codes over finite fields and rings have been investigated explicitly for the past few decades [1] [3] [4] [5] [6] [7] [8] [9] [10] [11].

3 Aim and Objectives of Research

The main objective of my research during Ph.D. is to elaborate the distance properties of linear codes:

(i) We will investigate and expand some parameters of linear codes such as length,

dimension, minimum distance and genrator matrix etc.

(ii) We will study Cyclic, Constacyclic, Quasi-cyclic, Negacyclic codes and their duals over finite fields and finite rings. We will also study bounds for these codes.

(iii) We will explore the distance properties of some of the codes listed in (ii) and study decoding techniques of these codes.

4 Methodology to be adopted

My area of research is theoretical in nature. Mostly, I will be referring the text books and research papers of various researchers who have developed this area of research. I would also like to consult with my thesis supervisor time to time to discuss the doubts. I would also like to participate in the schools, seminars, workshops in my area of research, which will help me to strengthen my knowledge in my field of research.

5 Importance of Study

The area of my research is highly applicable in coding theory. Coding theory has its origins in the engineering problem of effective electronic communication where the alphabet is generally the binary field. Since its inception, it has grown as a branch of Mathematics, and has since been expanded to consider any finite fields, and later also finite rings, as its alphabet. This proposal will presents a broad view of the subject and relates major results by ring theory.

6 Proposed Plan of Action

Following is the Year-wise plan of work and target to be achieved during my research period:

Year 1:

Course work and reading : I will complete the course work and other academic formalities declared by SRTMU Nanded in the first semester. Then after, I would like to read the text books [2] [14] [15] to develop necessary background for my research.

Year 2:

I would like to read the research papers , text books, and would like to complete research related literature survey and decide the problem for my PhD thesis in consultation with my thesis supervisor. I would also like to participate in various national and international workshops, schools and conferences to get the broader view and to develop academic relations with other research scholars.

Year 3:
I will focus on my research problem and would like to learn various techniques and methods by the other researchers on my area of research.
Year 4:
I will try to solve my thesis problem and try to have my publications related to my work.
Year 5:
I will try to write my thesis and submit to university for the award of PhD.

References

[1] Cao, Yonglin, *On constacyclic codes over finite chain rings,Finite Fields and Their Applications*, (2013).

[2] R. Lidl and H.Niederreiter, *Introduction to Finite Fields and Their Applications*, rev. ed. Cambridge, England: Cambridge University Press, (1994).

[3] B. Chen, Y. Fan, L. Lin and H. Liu, *Constacyclic codes over finite fields*, Finite Fields Appl,18, 1217–1231, (2012).

[4] Fengwei Li and Qin Yue and Fengmei Liu, *The weight distributions of constacyclic codes*, Advances in Mathematics of Communications, 11,3, 471-480, (2017).

[5] Li, F., Yue, Q. *The primitive idempotents and weight distributions of irreducible constacyclic codes*. Des. Codes Cryptogr. 86, 771–784 ,(2018).

[6] Minjia Shi, Alessandro Neri, Patrick Solé. *How many weights can a quasi-cyclic code have ?*. IEEE Transactions on Information Theory, Institute of Electrical and Electronics Engineers, 10.1109/TIT.2020.3001591. hal-02790988, (2020).

[7] K. Ding, C. Ding, *Binary linear codes with three weights*, IEEE Commun. Lett., 18, 1879– 1882, (2014).

[8] C. Ding, *The weight distributions of some irreducible cyclic codes*, IEEE Trans. Inf. Theory, 55 , 955–960, (2009).

[9] X. Huang, Q. Yue, Y. Wu, X. Shi, J. Michel, Binary *primitive LCD BCH codes, Design. Code.*Cryptogr., 88 , 2453–2473, (2020).

[10] Wang, X., Zheng, D and Liu, H. *Several classes of linear codes and their weight distributions*. AAECC 30, 75–92 (2019).

[11] Hai Q. Dinh,*Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*,Journal of Algebra,(2008)

[12] R. Hamming, *Error detecting and error correcting codes*. Bell Syst. Tech. J. 29, 147-160 (1950).

[13] C. Shannon, *A Mathematical Theory of Communication*. Bell Syst. Techn. J. 27 (1948).

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error Correcting Codes*, North Holland, Amsterdam, (1977).

[15] Ling and S Xing, *Coding theory: a first course*, Cambridge University Press, Chicago, (2004).

[16] Shixn zhu, Liqi Wang, *A class of constacyclic codes over* $\mathbb{F}_p$ *and* $v\mathbb{F}_p$ *and its Gray image*, Discrete Mathematics volume 311, issues 23-24, pages 2677-2682, (2011).

Mr.Sonkamble Rajesh Digambarrao
Research Student

Dr. Arun Baburao Jadhav
Research Guide